

# **Exhibit I**

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

EARNESTINE MATTHEWS,  
individually and on behalf of all others  
similarly situated,

Plaintiff,

vs.

UNITED RETAIL INCORPORATED,  
Defendant.

---

CASE NO. 07 C 02487

Judge Castillo

**DECLARATION OF JOEL S.  
LSKER IN OPPOSITION TO  
PLAINTIFF'S MOTION FOR  
CLASS CERTIFICATION**

JOEL S. LISKER makes the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746:

1. I am a consultant with the firm of Dudinsky Lisker & Associates, LLC. Prior to joining my current firm, I was Senior Vice-President for Security and Risk Management at MasterCard International, now MasterCard WorldWide, where I worked for 17 years. In this capacity I served as MasterCard International's worldwide senior security representative for all matters relating to the fraudulent use of its numerous card products. Moreover, I chaired the MasterCard International Security Committee for nine years from 1987 to 1996. It was the function of this committee which was comprised of senior security and risk management representatives of MasterCard's major members, to set all policies best practices and rules for the more than twenty thousand MasterCard member banks. A summary of my biographical information is attached as Exhibit A hereto.

2. During my tenure at MasterCard International, the Security and Risk Management department of the company was recognized by the Director of the United States Secret Service as the preeminent security department of the payments card industry. For example, MasterCard was first to develop and use the hologram as an overt security feature which technology was later imitated by our competitors. We were first to develop a tamper-evident signature panel upon which was placed a reverse italic, indent printed component of the account number together with a three digit value called CVC2 (Card Validation Code 2). The privilege to use this technology was extended by MasterCard to its competitors in the interest of reducing payments card industry fraud across all schemes. MasterCard was first to migrate to high coercivity magnetic stripe moving from 300 to 3200 Oersteds plus or minus ten percent. The standard was completed in 1999 and migrated to the U.S. and Europe in 2000 and to Asia in 2002. This enhancement of the magnetic stripe contributed to the reliability to the stripe read and a diminution of accidental erasure. MasterCard was first to build the merchant alert service (MATCH), fraud reporting system (SAFE), Risk Assessment Management Program (RAMP), a MasterCard alerts program to alert members of compromised accounts within a four hour time frame, numerous best practice programs ranging from preventing card fraud to dealing with mail contaminated by Anthrax, as well as the initiation with the American Bankers Association of a payments card industry fraud prevention program inclusive of representatives of all major brands. There were many other accomplishments too numerous to list.

3. I have been retained by DLA Piper US LLP on behalf of defendant United Retail Incorporated (“United Retail”) to address the issue of the risk, if any, to a cardholder that may result from the printing of the last five digits of the account number and an expiry date on a credit or debit card receipt.

4. I am being compensated for my services on this case at the rate of \$500 per hour.

5. I have given depositions in the following cases: STEPHEN CICILLINE JR., JAMES BATTERSON and CHRISTOPHER IOSELLO, individually and on behalf of a class, vs. JEWEL FOOD STORES, INC. d/b/a JEWEL-OSCO, a New York Corporation and Does 1-10, Case No. 07-C-2333, 07-C-2375, 07-C-2452. United States Court for the Northern District of Illinois, Eastern Division; Deposition Date: September 18, 2007.

KARL L. HALPERIN, individually and on behalf of a class, vs. INTERPARK, INC., and Does 1-10, Case No. 07 CV 216. United States Court for the Northern District of Illinois, Eastern Division; Deposition Date: October 2, 2007.

TJX Companies Retail Security Breach Litigation, Case No. 07-10162-WGY United States Court for the District of Massachusetts; Deposition Date: September 24, 2007.

I have written a piece as an Op Ed for Digital Transactions Magazine, entitled “Endpoint: Time to Overhaul the Drivers’ License” (November 2004).

6. I have reviewed the Answer and Defenses to Complaint-Class Action, Plaintiff’s Motion for Class Certification, Defendant United Retail Incorporated’s Objections and Responses to Plaintiff’s First Set of Interrogatories, Memorandum in Support of Plaintiff’s Motion for Class Certification, Defendant United Retail Incorporated’s Rule 26(a)(1) Initial Disclosures, Agreed Protective Order, Plaintiff’s Rule 26(a)(1) Disclosures, and an “Avenue” receipt in the amount of \$16.00 drawn on December 15, 2006.

7. It is my opinion that the fact that last five digits of the credit card account number and an expiry date were printed on the unredacted copy of plaintiff’s receipt did not expose plaintiff to any risk of harm from identity theft or payment card fraud-for the reasons described below. Moreover, the absence of the name of the cardholder on the receipt would render the last five digits of the

account number and the expiry date superfluous and without value for purposes of perpetrating credit card fraud in any respect.

8. A debit or credit card expiry date is neither generally necessary, nor alone sufficient for charges to be made to plaintiff's account. First, there can be no charges to plaintiff's account without the exact credit or debit card number. This number is not present on the plaintiff's receipt. Second, if an unauthorized individual gains access to plaintiff's exact credit or debit card account number, the unauthorized individual could not engage in a card-not-present transaction, whether on the phone or via the internet without information beyond that found on plaintiff's receipt, such as the Card Validation Code 2 (CVC2) or in the case of Visa CVV2, and the cardholder's "bill to address" which may be verified by the issuer through the Address Verification Service (AVS). In any event, the unauthorized individual would generally have no need for the expiry date, because at this time there is no requirement under the VISA and MasterCard rules that an expiry date be verified as a condition of authorization, and, indeed absent extraordinary circumstances, card issuers generally do not verify the expiry date at the time of the authorization of the transaction so long as the date is not past and is less than 20 years hence.

9. Actual "identify theft", as that term is generally understood, is something different than mere fraudulent charges on a credit or debit card. The two are in no respect synonymous and the only relationship exists wherein after an "identity has been taken over" by a criminal, that criminal attempts to open accounts in the name of the victim. This enabling information can result from phishing, database compromises, credit bureau compromises and similar actions resulting from several sources. It may take months or even years before a victim learns of the crime perpetrated against them, and even longer to expunge the fraud from credit reports. This is because in many cases the financial institution believes its customer (cardholder) is simply undergoing financial difficulties unrelated to

actual fraud. Such identity theft has no relation to the printing of an expiry date on a payment card receipt and, an identity thief bent on perpetrating such a scheme would find no significant incremental value in obtaining payment card expiry date.

10. To attempt to equate identify theft with credit card fraud and regard them as synonymous flies in the face of common sense and business practices. It is completely at odds with both MasterCard and VISA rules. For example, under MasterCard rules there are several categories of fraud divided into three tiers. The tiers are indicative of time reporting requirements. Tier I categories of fraud to be reported by issuers in the MasterCard system are: lost, stolen, never received issued (NRI), and counterfeit. The Tier II category is card not present (CNP). The Tier III category includes: fraudulent applications, account takeover and multiple imprints. So clearly, these are eight discrete categories of fraud, not simply one labeled “identity theft.” Moreover, few of these categories with the exception of account takeover are even related to identity theft. Finally to my knowledge, out of the millions of transactions in which card issuers experience fraud, not a single one has ever resulted from the use of an expiry date together with the last four or five digits of a truncated account number.

11. The General Accountability Office in its June 2007 report titled “Personal Information, Data Breaches are Frequent, but Evidence of Identity Theft is Limited; However, the Full Extent is Unknown,” (excerpts attached as Exhibit B, hereto) at page 30, the GAO report correctly observed that “The type of data compromised in a breach can effectively determine the potential harm that can result. For example, credit or debit card information such as card numbers and expiration dates generally cannot be used alone to open unauthorized new accounts. Some of the largest and most highly publicized data braches in recent years largely involved credit or debit card data rather than personally identifiable information. As a result, these breaches put affected consumers at risk of account fraud but not necessarily at risk of fraud involving unauthorized creation of new accounts—the

type of identity theft generally considered to have more harmful direct effect on consumers. While credit and debit card fraud is a significant problem—the FTC estimates it results in billions of dollars in losses annually—existing laws limit consumer liability for such fraud and, as a matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges. In contrast, the unauthorized creation of new accounts—such as using someone else’s identity to open credit card or bank accounts, originate home mortgages, file tax returns, or apply for government benefits—can result in substantial financial costs and other hardships.” The “billions of dollars in losses” referenced in the GAO Report are not losses to cardholders, but losses to the banking institutions that issue the cards or the acquirers that process the merchants’ accounts or the merchants themselves. These are the entities who bear the loss for fraudulent credit card use, as discussed in the ensuing paragraphs. Because of this risk, these entities have devoted significant resources to its mitigation, which efforts continue to this day. Some of these efforts are described above in paragraph two.

12. Even if somehow fraudulent charges were made to a cardholder’s account, the cardholder would not be at risk of any loss in any reasonable scenario. Under Regulation Z under the Truth in Lending Act, 12 CFR ¶ 27-712 (excerpt attached as Exhibit C), a credit card holder’s liability cannot exceed the lesser of \$50 or the amount of fraudulent charges made in person by the thief before notification to the card issuer. Thus, regardless of how long it takes the cardholder to notify the bank, his or her maximum legal liability is \$50. Moreover, as a matter of policy neither MasterCard nor Visa issuers will assess the \$50 charge against an innocent cardholder.

13. Debit cards are governed by Regulation E Truth in Lending Act, 12 CFR ¶ 27-406 (excerpt attached as Exhibit D). In cases of fraudulent use of a debit card (where the card itself was not lost or stolen), Section 205.6(b)(3) within Regulation E provides as follows: The consumer must report the unauthorized use

within 60 days of the date when the bank transmitted the bank statement with the initial fraudulent charges in order to avoid liability for *subsequent* unauthorized transfers of money out of the consumer's account. If the consumer reports an unauthorized use within this 60-day period, the consumer has no legal liability for the unauthorized charges.

14. Even the remote financial risk exposures described above, however, have been eliminated by virtue of card association practices, pursuant to which the card associations have adopted "no liability" policies with respect to both debit and credit card use that relieves the cardholder from any liability for fraudulent charges. Thus, neither a debit card nor credit card holder has any practical exposure to any risk from fraudulent card use.

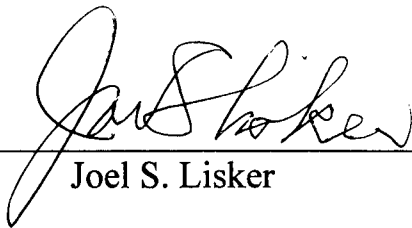
15. Finally, in the instant case, if a thief were in possession of the last five digits of the account number together with the expiry date and the name of the payment card franchise (American Express, Diners, Visa, MasterCard, Discover) the thief would in effect have six digits (inclusive of the first) American Express, Diners (3), Visa (4), MasterCard (5), Discover (6). If armed with this data, the thief attempted to enter multiple permutations of the remaining missing account digits the thief would encounter the issuer's risk control apparatus encompassing a neural network, rules based fraud detection system or a hybrid of the two. After multiple unsuccessful tries, the failure of the Mod 10 check digit to verify sequence of the numbers entered would result in an alert being generated, so that any transaction utilizing those numbers encompassing the sequence of the last five digits of the account number would result in a queuing of the aborted transaction and an investigation would be undertaken to contain potential fraud exposure.

16. Moreover, in a card-not-present (CNP) transaction, in most cases, the fraud risk lies with the merchant and such merchants have often developed their own fraud detection capabilities to mitigate their potential risk. For example, merchants will verify a cardholder's "bill to address" utilizing the

Address Verification Service (AVS) of MasterCard and others for certain classes of goods such as airline tickets, theater tickets and other high value items such as cell phones, computers, technical components, etc.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 26, 2007.



---

Joel S. Lisker

# Exhibit A

## **EXHIBIT A**

### **JOEL S. LISKER**

Mr. Joel S. Lisker was most recently the Senior Vice-President for Security and Risk Management for MasterCard International. In this capacity he served as the company's world-wide senior security representative for all matters relating to the fraudulent use of its numerous card products. He was instrumental in developing technical solutions and strategies to thwart the efforts of organized crime, and as head of Corporate Security with responsibility for safeguarding MasterCard employees, premises, and property throughout the world, he ensured the safety and security of its' human and physical assets, without incident. At MasterCard, he led the development of chip-based biometrics solutions for data security, perimeter security, visitor screening and employee authentication.

As the senior security risk official for MasterCard International he chaired the MasterCard International Security Committee for nine years from 1987 to 1996. Moreover, it was the function of this committee, comprised of senior security and risk management representatives of MasterCard's major members, to set all policies best practices and rules for the more than twenty thousand MasterCard members banks. He has also established and served on the American Bankers Association (ABA) payment systems security committee that was comprised of the senior security and risk senior managers from MasterCard, Visa, American Express, Diners, Discover and JCB. This committee developed common strategies to impact fraudsters who struck at the various payment systems without regard to brand.

He has also worked extensively on standards with ISO and ANSI, testified in 38 criminal trials as the FBI's forensic document expert in Federal and state Courts. These cases involved everything from check forgery to mass homicide.

He has testified several times, in conjunction with his counterparts from Visa and American Express before the House and Senate Committees and subcommittees with jurisdiction over legislation, agencies and regulations involving payment cards.

Mr. Lisker has addressed as a keynote or principal speaker, or as panel chair scores of meetings of the IAFCI, the Biometric Consortium, CardTecSecure Tec MasterCard regional meetings here and abroad, Interpol, FBI, the Federal

Reserve, FDIC, European Commission, G-8, Independent Commission Against Corruption, etc.

He has served and currently serves on 3 corporate Advisory Boards and 1 corporate Board of Directors. Each of these companies has products or services that impact fraud, account takeover, identity theft or deception.

After completion of his formal education at the University of Pennsylvania (B.S.) and the Temple University School of Law (J.D.), he joined the FBI as a Special Agent where he worked against domestic terrorist groups. Thereafter, as a Special Agent Supervisor, assigned to FBI Headquarters, he developed sophisticated solutions to safeguard FBI communications between FBI Headquarters and its' overseas offices. He also developed techniques used in foreign counter-intelligence operations.

Next, Mr. Lisker served as senior trial Attorney in the U.S. Dept. of Justice Criminal Division, Internal Security section where he directed a task force operating against domestic terrorists, and led a group seeking to discover and control foreign agents.

In 1981, Mr. Lisker was selected by the Chairman of the U.S. Senate Committee on the Judiciary, to be Chief Counsel and Staff Director of its' newly formed Sub-Committee on security and terrorism. In addition to managing the Committee's oversight and authorization responsibility for the FBI, the DEA and the U.S. Marshal Service, he has organized more than 35 hearings aimed at uncovering the global terrorist inter-connections and transnational operations that became known as the "terror network". Mr. Lisker was also responsible for drafting legislation with respect to protecting identities of covert agents, jurisdictional realignment of authority regarding escaped federal prisoners and other fugitives from justice, criminalization of payments card fraud and counterfeit, amendment of legislation relating to agents of foreign principals, etc.

In each of his roles and in the responsibilities he was required to carry out over the years Mr. Lisker has maintained regular contact with counterparts in the FBI and those reporting to the Director of Central Intelligence. In 1987, Mr. Lisker was selected as Associate Counsel to the Senate select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition. One of his major accomplishments in this assignment was the uncovering and tracing of clandestine funding sources, through the Swiss banking Network.

Mr. Lisker is a member of the District of Columbia Bar, and is admitted to practice before the U.S. District Court and the U.S. Court of Appeals for the District of Columbia Circuit. He is also admitted to practice before the U.S.

Supreme Court. He is a life member of the FBI Agents Association, The Association of Former Agents of the FBI. He serves on several corporate Boards of Directors and Advisory Boards and is currently serving on two FBI industry Task Forces dealing with Terrorist Financing and Identity Theft.

Mr. Lisker brings to Dudinsky Lisker & Associates, LLC current, wide ranging, and state of the art experience in biometric technologies, neural network technologies, and other cutting edge risk reduction solutions.

# **Exhibit B**

June 2007

# PERSONAL INFORMATION

Data Breaches Are  
Frequent, but  
Evidence of Resulting  
Identity Theft Is  
Limited; However, the  
Full Extent Is  
Unknown



G A O

Accountability \* Integrity \* Reliability



Highlights of [GAO-07-737](#), a report to congressional requesters

## Why GAO Did This Study

In recent years, many entities in the private, public, and government sectors have reported the loss or theft of sensitive personal information. These breaches have raised concerns in part because they can result in identity theft—either account fraud (such as misuse of credit card numbers) or unauthorized creation of new accounts (such as opening a credit card in someone else's name). Many states have enacted laws requiring entities that experience breaches to notify affected individuals, and Congress is considering legislation that would establish a national breach notification requirement.

GAO was asked to examine (1) the incidence and circumstances of breaches of sensitive personal information; (2) the extent to which such breaches have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. To address these objectives, GAO reviewed available reports on data breaches, analyzed 24 large data breaches, and gathered information from federal and state government agencies, researchers, consumer advocates, and others.

## What GAO Recommends

This report contains no recommendations.

[www.gao.gov/cgi-bin/getrpt?GAO-07-737](http://www.gao.gov/cgi-bin/getrpt?GAO-07-737).

To view the full product, including the scope and methodology, click on the link above. For more information, contact David G. Wood at (202) 512-8678 or [woodd@gao.gov](mailto:woodd@gao.gov).

# PERSONAL INFORMATION

## Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

### What GAO Found

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches were reported in the news media from January 2005 through December 2006, according to lists maintained by private groups that track reports of breaches. These incidents varied significantly in size and occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities.

The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts. For example, in reviewing the 24 largest breaches reported in the media from January 2000 through June 2005, GAO found that 3 included evidence of resulting fraud on existing accounts and 1 included evidence of unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, there was not sufficient information to make a determination.

Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges. Notification requirements can create incentives for entities to improve data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach. Also, consumers alerted to a breach can take measures to prevent or mitigate identity theft, such as monitoring their credit card statements and credit reports. At the same time, breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals. Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether. Federal banking regulators and the President's Identity Theft Task Force have advocated a notification standard—the conditions requiring notification—that is risk based, allowing individuals to take appropriate measures where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Results in Brief	5
	Background	7
	Available Evidence Indicates That Data Breaches Occur Frequently and Under Varying Circumstances	10
	Consequences of Data Breaches Are Not Fully Known, but Clear Evidence of Identity Theft Has Been Found in Relatively Few Breaches	21
	Breach Notification Requirements Can Serve to Encourage Better Data Security Practices and Alert Consumers, but They Also Present Costs and Challenges	31
	Agency Comments	40
<b>Appendix I</b>	<b>Scope and Methodology</b>	<b>42</b>
<b>Appendix II</b>	<b>GAO Contact and Staff Acknowledgments</b>	<b>45</b>
	GAO Contact	45
	Staff Acknowledgments	45
<b>Table</b>		
	Table 1: Twenty-Four Large Publicly Reported Data Breaches and Evidence of Resulting Identity Theft, January 2000 - June 2005	26
<b>Figure</b>		
	Figure 1: Application of Notification Standards under Different Breach Scenarios	37

---

## Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FTC	Federal Trade Commission
SSN	Social Security number
USPIS	United States Postal Inspection Service
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

June 4, 2007

The Honorable Spencer Bachus  
Ranking Member  
Committee on Financial Services  
House of Representatives

The Honorable Michael N. Castle  
House of Representatives

The Honorable Darlene Hooley  
House of Representatives

The Honorable Steven C. LaTourette  
House of Representatives

The Honorable Dennis Moore  
House of Representatives

As a result of advances in computer technology and electronic storage, many different sectors and entities now maintain electronic records containing vast amounts of personal information on virtually all American consumers. In recent years, a number of entities—including financial service firms, retailers, universities, and government agencies—have collectively reported the loss or theft of large amounts of sensitive personal information. Some of these data breaches—such as those involving TJX Companies and the Department of Veterans Affairs (VA)—have received considerable publicity and have highlighted concerns about the protections afforded sensitive personal information.<sup>1</sup> Policymakers, consumer advocates, and others have raised concerns that data breaches can contribute to identity theft, in which an individual's sensitive personal

---

<sup>1</sup>In January 2007, The TJX Companies, Inc., publicly disclosed a data breach that compromised sensitive personal information, including credit and debit card data, associated with more than 45 million customer accounts. In May 2006, VA reported that computer equipment containing sensitive personal information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised. See GAO, *Privacy: Lessons Learned About Data Breach Notification*, [GAO-07-657](#) (Washington, D.C.: Apr. 30, 2007).

---

information is used fraudulently. The Federal Trade Commission (FTC), which is responsible for taking complaints from victims and sharing them with law enforcement agencies, has noted that identity theft is a serious problem—millions of Americans are affected each year, and victims may face substantial costs and time to repair the damage to their good name and credit record.

Although there is no commonly agreed-upon definition, the term “data breach” generally refers to an organization’s unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers.<sup>2</sup> Data breaches can take many forms and do not necessarily lead to identity theft. The term “identity theft” is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else’s name. Depending on the type of information compromised and how it is misused, identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings.

Beginning with California in 2002, at least 36 states have enacted breach notification laws—that is, laws that require certain entities that experience a data breach to notify individuals whose personal information was lost or stolen. There is no federal statute that requires most companies or other entities to notify affected individuals of data breaches, although federal banking regulatory agencies have issued guidance on breach notification

---

<sup>2</sup>In this report we use “personally identifiable information” to refer to any information that can be used to distinguish or trace an individual’s identity—such as name, Social Security number, driver’s license number, and mother’s maiden name—because such information generally may be used to establish new accounts, but not to refer to other “means of identification,” as defined in 18 U.S.C. § 1028(7), including account information such as credit or debit card numbers.

---

to the banks, thrifts, and credit unions they supervise.<sup>3</sup> In addition, the Office of Management and Budget has issued guidance—developed by the President’s Identity Theft Task Force—on responding to data breaches at federal agencies.<sup>4</sup> Because a number of bills have been introduced in Congress that would establish a national breach notification requirement, you asked us to review the costs and benefits of such a requirement and the link between data breaches and identity theft.<sup>5</sup> As agreed with your offices, this report examines (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements.

This report focuses on breaches of sensitive personal data that can be used to commit identity theft, and not on breaches of other sensitive data, such as medical records or proprietary business information. To address the first two objectives, we obtained and analyzed information on data breaches that have been reported in the media and aggregated by three

---

<sup>3</sup>See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005). The five federal banking regulatory agencies are the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. The National Credit Union Administration issued its guidance (which was substantially identical) separately from the other four regulators (see Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, 70 Fed. Reg. 22764 (May 2, 2005)).

<sup>4</sup>The President’s Identity Theft Task Force—chaired by the Attorney General and cochaired by the Chairman of the Federal Trade Commission and comprising 17 federal agencies and departments—was charged with developing a comprehensive national strategy to combat identity theft. Exec. Order No. 13,402, *Strengthening Federal Efforts to Protect Against Identity Theft*, 71 Fed. Reg. 27945 (May 10, 2006). The task force’s guidance was distributed in a memorandum from the Office of Management and Budget to the heads of federal agencies and departments. See Office of Management and Budget Memorandum for the Heads of Departments and Agencies, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006. In May 2007, the Office of Management and Budget issued a memorandum that updated the September 2006 guidance and, among other things, required agencies to develop and implement breach notification policies within 120 days. See Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007).

<sup>5</sup>See, for example, Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); and Identity Theft Prevention Act, S. 1178, 110th Cong. (2007).

---

private research and advocacy organizations, as well as information on breaches collected by state agencies in New York and North Carolina, federal banking regulators, and federal law enforcement agencies.<sup>6</sup> We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee in 2006 and by the Department of Homeland Security (DHS).<sup>7</sup> In addition, we conducted a literature search of relevant articles, reports, and studies. We also conducted interviews with, and obtained documents from, representatives of federal agencies, including the FTC, the Department of Justice, DHS, and the federal banking regulatory agencies; selected state government agencies and the National Association of Attorneys General; private and nonprofit research organizations; and consumer protection and privacy advocacy groups. Further, we obtained information from industry and trade associations representing key sectors—including financial services, retail sales, higher education, health care, and information services—that have experienced data breaches. In addition, for the second objective, we examined the 24 largest (in terms of number of records breached) data breaches reported by the news media from January 2000 through June 2005 and tracked by private groups. For each of these breaches, we reviewed media reports and other publicly available information, and conducted interviews, where possible, with representatives of the entities that experienced the breaches, in an attempt to identify any known instances of identity theft that resulted from the breaches. We also examined five breaches that involved federal agencies, which were selected because they represented a variety of different circumstances. For the third objective, we reviewed the federal banking regulatory agencies' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law, which included interviewing and gathering information from California

---

<sup>6</sup>The three private organizations are Attrition, Identity Theft Resource Center, and Privacy Rights Clearinghouse. We reviewed data on breaches in New York and North Carolina because they represent two large states that maintain centralized information on data breaches.

<sup>7</sup>The House Government Reform Committee was renamed the House Oversight and Government Reform Committee in the 110th Congress.

---

state officials and selected California companies, educational institutions, and other entities subject to the law's notification requirements.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards. A more extensive discussion of our scope and methodology appears in appendix I.

---

## Results in Brief

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches have been reported in the news media from January 2005 through December 2006, according to our analysis of lists maintained by three private organizations that track such breaches. Further, a House Government Reform Committee survey of federal agencies identified more than 788 data breaches at 17 agencies from January 2003 through July 2006. Of the roughly 17,000 federally supervised banks, thrifts, and credit unions, several hundred have reported data breaches to their federal regulators over the past 2 years. In addition, officials in New York State—which requires public and private entities to report data breaches to a centralized source—reported receiving notice of 225 breaches from December 7, 2005, through October 5, 2006. Data breaches have occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Some studies indicate that most publicly reported breaches resulted from intentional actions, such as a stolen laptop computer, rather than accidental occurrences, such as a lost laptop computer, but this may be because breaches related to criminal activity are perhaps more likely to be reported. Media-reported breaches have varied significantly in size, ranging from 10 records to tens of millions of records. Most of these breaches have compromised data that included personally identifiable information, while others have involved only account information such as credit card numbers.

The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the data used to commit identity theft. Although we identified several cases where breaches reportedly have resulted in identity theft—that is, account fraud or unauthorized creation of new accounts—available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, our review of the 24 largest

---

breaches that appeared in the news media from January 2000 through June 2005 found that 3 breaches appeared to have resulted in fraud on existing accounts, and 1 breach appeared to have resulted in the unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, we did not have sufficient information to make a determination. Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and it may be up to a year or more before stolen data are used to commit a crime. Some studies by private researchers have found little linkage between data breaches and identity theft, although our review found these studies had methodological limitations. Finally, the circumstances of a breach can greatly affect the potential harm that can result. For example, unauthorized creation of new accounts generally can occur only when a breach includes personally identifiable information. Further, breaches that are the result of intentional acts generally are considered to pose more risk than accidental breaches, according to federal officials.

Requiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft, but it also involves monetary costs and challenges such as determining an appropriate notification standard. Representatives of federal banking regulators, other government agencies, industry associations, and other affected parties told us that breach notification requirements have encouraged companies and other entities to improve their data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach of customer data. Further, notifying affected consumers of a breach gives them the opportunity to mitigate potential risk—for example, by reviewing their credit card statements and credit reports, or placing a fraud alert on their credit files. Some privacy advocates and others have noted that even when the risk of actual financial harm is low, breach notification is still important because individuals have a basic right to know how their personal information is being handled and when it has been compromised. At the same time, affected entities incur monetary costs to comply with notification requirements. For example, 31 companies that responded to a 2006 survey said they incurred an average of \$1.4 million per breach, for costs such as mailing notification letters, call center expenses, courtesy discounts or services, and legal fees. In addition, organizations subject to notification requirements told us they face several challenges, including the lack of clarity in some state statutes about when a notification is required, difficulty identifying and locating affected individuals, and difficulty

---

complying with varying state requirements. Notification standards—that is, the circumstances surrounding a data breach that “trigger” the required notification—vary among the states. Some parties, such as the National Association of Attorneys General, have advocated that a breach notification requirement should apply broadly in order to give consumers a greater level of protection and because the risk of harm is not always known. The guidance provided by federal banking regulators lays out a more risk-based approach, aimed at ensuring that affected individuals receive notices only when they are at risk of identity theft or other related harm. Such an approach was also adopted by the President’s Identity Theft Task Force, which recommended a risk-based standard for breach notification applicable to both government agencies and private entities. As we have noted in the past, care is needed in defining appropriate criteria for incidents that merit notification. Should Congress choose to enact a federal breach notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

This report contains no recommendations. We provided a draft of this report to FTC and provided selected portions of the draft to federal banking regulatory agencies and relevant federal law enforcement agencies. These agencies provided technical comments, which we have incorporated in this report as appropriate.

---

## Background

Breaches of sensitive personal data in recent years at companies, universities, government agencies, and other organizations have heightened public awareness about data security and the risks of identity theft, and have led to the introduction of breach notification requirements in many state legislatures. As of April 2007, at least 36 states had enacted some form of law requiring that affected individuals be notified in the event of a data breach; California’s law, enacted in 2002, was the first such state requirement.<sup>8</sup> States’ notification requirements vary, particularly with regard to the applicable notification standard—the event or circumstance that triggers a required notification. Requirements also vary in terms of the data to which they apply—for example, some apply to paper documents as well as electronic records.

---

<sup>8</sup>Cal. Civ. Code § 1798.82.

---

## Consequences of Data Breaches Are Not Fully Known, but Clear Evidence of Identity Theft Has Been Found in Relatively Few Breaches

Comprehensive information on the outcomes of data breaches is not available. Several cases have been identified in which a data breach appears to have resulted in identity theft, but available data and information from law enforcement and industry association representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, of 24 very large breaches we reviewed, 3 appeared to have resulted in fraud on existing accounts and 1 in the unauthorized creation of new accounts. Determining the link between data breaches and identity theft is challenging because, among other things, identity theft victims often do not know how their personal information was obtained. However, the circumstances of a breach, including the type of information compromised and how the breach occurred, can greatly affect the potential risk of identity theft.

---

## Federal Law Enforcement Agencies and Industry Associations Identified Limited Instances of Breaches Leading to Identity Theft

In general, representatives of law enforcement agencies, industry and trade associations, and consumer and privacy advocacy organizations told us that no comprehensive data are available on the consequences of data breaches. Several cases have been identified where there is evidence that a data breach resulted in identity theft, including account fraud or unauthorized creation of new accounts. At the same time, available data and information from the officials we contacted indicated that most breaches have not resulted in detected incidents of identity theft.

We asked representatives of the FBI, Secret Service, USPIS, and Immigration and Customs Enforcement—a component of DHS that has investigated cases where stolen identities were used to secure jobs—the extent to which data breaches they investigated resulted in some form of identity theft. Representatives of all of these agencies told us that their investigations of data breaches do not typically allow them to fully ascertain how stolen data are used. Similarly, they noted that investigations of identity theft do not always reveal the source of the data used to commit the crime.

However, the representatives were able to provide us with a limited number of examples in which data breaches they investigated had allegedly resulted in some form of identity theft. For example, in a 2006 investigation by USPIS, an employee of a credit card call center allegedly compromised at least 35 customers' accounts and used some of the information to purchase approximately \$65,000 in gift cards. The representatives of federal law enforcement agencies noted that cases in which data breaches have been linked to identity theft often have involved instances of unauthorized access by employees. For example, an official at

---

Immigration and Customs Enforcement stated that her agency, in cooperation with other agencies, has investigated cases in which government employees allegedly had improperly accessed and sold sensitive personal information that was then used by illegal immigrants to secure employment.

In addition, in 2005 FTC settled charges with BJ's Wholesale Club in which alleged security breaches resulted in several million dollars in fraudulent purchases using customers' credit and debit card data.<sup>38</sup> As discussed later in this report, FTC has also taken enforcement actions related to data breaches at several other companies, including ChoicePoint, CardSystems, and DSW, in which it uncovered evidence that the breaches resulted in identity theft.

Many of the law enforcement officials said that, based on their experience, data breaches that result in harm have usually involved fraud on existing accounts (such as credit card fraud) rather than the unauthorized creation of new accounts. Secret Service representatives noted that using illicit credit and debit card numbers and bank account information is much easier and less labor intensive than using personally identifiable information to fraudulently open new accounts. Officials at Secret Service, FBI, and USPIS all said that identity theft involving the creation of new accounts often results not from data breaches, but from other sources, such as retrieving personal information by sifting through a family's household trash.

In examining a selection of five breaches that occurred from 2003 through 2005 that were reported as having involved five federal agencies—Department of Justice, FDIC, Internal Revenue Service, National Park Service, and the Navy—we found that the circumstances behind these breaches varied widely. At least two of the breaches occurred at vendors or contractors that held sensitive data on agency employees, rather than at the agency itself. In addition, we found that a breach reported in the news media as having involved the National Park Service actually involved a not-for-profit organization that manages eParks, according to a representative of that organization. Four of the five breaches reported as having involved federal agencies were not believed to have resulted in identity theft, according to officials of the entities involved. The breach at

---

<sup>38</sup>*In the Matter of BJ's Wholesale Club, Inc.*, F.T.C. No. 0423160 (2005). A consent agreement does not constitute an admission of a violation of law.

---

FDIC resulted in an estimated 27 cases of identity theft when data inappropriately accessed by a former FDIC intern were used to take out more than \$425,000 in fraudulent loans in the names of FDIC employees, according to agency officials.<sup>39</sup>

Industry and trade associations representing entities that maintain large amounts of information—banks, retailers, colleges, information resellers, and hospitals—told us that they had limited knowledge about the harm caused by data breaches that occur in their industries. However, in some cases, they provided information or anecdotal evidence on the extent to which such breaches may have led to some form of identity theft. For example, the 46 hospitals that the American Hospital Association surveyed at our request reported that of 17 breaches that had occurred since 2003, three had resulted in fraudulent activity on existing accounts and another three resulted in other forms of identity theft, including one case where the information was used to file false income tax refunds. The identity theft in these cases involved small numbers of victims—usually just one.

Representatives of the American Council on Education and two other higher education associations stated that while data breaches at colleges and universities were not uncommon, they were aware of little to no identity theft that had resulted from such breaches. Representatives of the American Bankers Association, the National Retail Federation, and the Consumer Data Industry Association told us they were unable to determine how prevalent data breaches are among their institutions or how often such breaches lead to consumer harm. Representatives at the National Retail Federation noted that breaches at retailers may be more likely to result in fraud on existing accounts than in new account creation, since most retailers do not maintain the personally identifiable information needed to steal someone's identity.

---

<sup>39</sup> According to an FDIC representative, the agency took several steps to address the possible misuse of employee information, including promptly notifying affected employees and offering them 2 years of credit monitoring services.

---

## Of 24 Large Publicly Reported Breaches, 4 Apparently Resulted in Known Cases of Identity Theft

Using lists of data breaches compiled by the Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service, we identified the 24 largest breaches (measured by number of records) that were reported in the news media from January 2000 through June 2005.<sup>40</sup> To gather information on these incidents, we interviewed or collected written responses from representatives of the entity experiencing the breach and reviewed publicly available information, such as media reports, news releases, testimonies, and court documents. In some cases, when feasible, we also spoke with law enforcement investigators. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts.

Although these lists characterized each of these 24 incidents as data breaches, the circumstances of the incidents varied. While 19 of the incidents clearly met our definition of data breach (i.e. unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information), four cases involved hackers who may or may not have actually accessed sensitive information. In one other incident, a university employee with access to sensitive personal data was indicted on unrelated fraud charges. A university official told us he did not believe this incident should necessarily be characterized as a data breach since there was no evidence the employee actually misused university data.

The available evidence that we reviewed indicated that 18 of these 24 breaches were not known to have resulted in any identity theft. As shown in table 1, three breaches were believed to have resulted in account fraud and one resulted in the unauthorized creation of new accounts. In two

---

<sup>40</sup>These three organizations periodically update their lists by adding breaches they learn about that occurred in the past, including some that occurred between January 2000 and June 2005. Our list of the 24 largest media-reported breaches was based on information provided by these lists as of August 2006. We were not aware of the Attrition list at the time we made our selection. See Congressional Research Service, *Personal Data Security Breaches: Context and Incident Summaries*, Order Code RL33199 (Washington, D.C.: Dec. 16, 2005). Because our time frame covered only breaches that occurred on or before June 30, 2005, our list does not include highly publicized breaches that occurred subsequently, such as those involving the Department of Veterans Affairs and the TJX Companies. Several banks have reported fraudulent transactions on existing accounts resulting from the TJX breach, according to a January 24, 2007, press release by the Massachusetts Bankers Association.

---

other cases, we were not able to gather sufficient information on whether harm appeared to have resulted from the breach. Further, because of the challenges in linking data breaches with identity theft, in some cases our review may not have uncovered instances of harm potentially resulting from these breaches. In some instances, investigators or company representatives reported that they were able to determine with a high degree of certainty—through forensic investigation or other means—that unauthorized parties had not accessed the data. In other instances, these representatives said that they were not aware of any account fraud that resulted, but they acknowledged that there was no way to know for sure. Moreover, determining potential harm may be particularly challenging with very large breaches because the volume of records involved can make it difficult to link individual victims to the breach.

**Table 1: Twenty-Four Large Publicly Reported Data Breaches and Evidence of Resulting Identity Theft, January 2000 - June 2005**

The fact that we did not identify evidence of identity theft from a breach does not necessarily mean that no such harm has occurred or will occur in the future.

Year <sup>a</sup>	Type of organization	Nature of breach	Available evidence of identity theft? <sup>b</sup>
2000	Retail	Hacking	Account fraud
2000	Retail	Hacking	None identified
2002	Healthcare	Stolen computer equipment	None identified
2003	Higher education	Stolen computer equipment	None identified
2004	Financial services	Stolen computer equipment	None identified
2004	Higher education	Hacking	None identified
2004	Higher education	Hacking	None identified
2004	Higher education	Hacking	None identified
2004	Financial services	Lost data tapes	None identified
2005	Financial services	Hacking	Account fraud
2005	State government	Hacking	None identified
2005	Information services	Deception/Misrepresentation	Unauthorized new accounts
2005	Higher education	Hacking	None identified
2005	Higher education	Stolen computer equipment	None identified
2005	Retail	Hacking	Account fraud
2005	Information services	Deception/Misrepresentation	Unknown
2005	Healthcare	Stolen computer equipment	None identified
2005	Retail	Hacking	Unknown
2005	Financial services	Lost data tapes	None identified
2005	Financial services	Employee crime	None identified
2005	State government	Hacking	None identified
2005	Media	Lost data tapes	None identified
2005	Financial services	Lost data tapes	None identified
2005	Higher education	Other <sup>c</sup>	None identified

Source: GAO.

Note: To identify the 24 largest data breaches reported in the news media from January 2000 through June 2005, GAO analyzed lists of such breaches maintained by Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service.

<sup>a</sup>Year breach occurred or was publicized.

---

<sup>b</sup>The presence or lack of evidence of identity theft resulting from a breach was based on our review of news reports and other publicly available information, as well as interviews, as feasible, with representatives of entities experiencing the breach and law enforcement officials investigating the breach. The fact that we were unable to identify evidence at this time of identity theft resulting from a breach does not mean that no such harm has occurred or that none will occur in the future. Further, factual determinations of the existence and cause of identity theft in any particular case are matters for the courts to decide.

<sup>c</sup>In this case, a former university employee with access to sensitive personal information had been indicted on bank fraud charges unrelated to the university. Some press reports characterized this as a breach, but according to a representative of the university, there is no evidence that the employee misused university data.

The one large breach we identified that apparently resulted in the unauthorized creation of new accounts involved ChoicePoint, an information reseller. In 2005, the company acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services. FTC reached a civil settlement in 2006 with the company that established a fund for consumer redress to reimburse potential victims of identity theft, and the agency has worked with law enforcement officials to identify such victims.<sup>41</sup>

The three large breaches we identified that appeared to result in fraud on existing accounts included the following:

- CardSystems, a credit card payment processor, reported a May 2005 breach in which a hacker accessed data such as names, card account numbers, and expiration dates. The total number of compromised accounts is unclear. FTC staff alleged in a 2006 civil complaint that the breach had compromised data associated with tens of millions of credit and debit cards, but a CardSystems official stated in congressional testimony that only 239,000 accounts were compromised. Officials of the Office of the Comptroller of the Currency—who surveyed the national banks they supervise in order to determine the amount of fraudulent charges that resulted from the breach—said that customers of 110 banks were affected by this incident and losses of more than \$13

---

<sup>41</sup>*United States v. ChoicePoint, Inc.*, No. 1:06-cv-00198-JTC (N.D. Ga., Feb. 15, 2006). As part of the settlement, ChoicePoint admitted no violations of the law. According to ChoicePoint, the company has subsequently taken steps to enhance its customer screening process and to assist affected consumers. FTC staff told us that law enforcement officials have determined that as many as 2,900 people have experienced the fraudulent creation of new accounts as a result of the breach. According to a ChoicePoint official, the criminal indictments indicated that 46 people may have been defrauded, but the accused individuals may not have used data acquired from ChoicePoint in all the crimes cited in the indictments.

---

million in fraudulent charges on customers' cards were reported by 24 of these institutions.

- DSW, a shoe retailer, said in an April 2005 news release that it had experienced a data breach in which a hacker accessed the names and card numbers associated with 1.4 million credit and debit card transactions at 108 of its stores, as well as checking account numbers and driver's license numbers from 96,000 check transactions. According to a complaint filed by FTC in March of 2006, there allegedly have been fraudulent transactions on some of these accounts.
- CD Universe, an Internet-based music store, reportedly experienced a breach in December 1999 in which a hacker accessed as many as 300,000 names, addresses, and credit card numbers from the company Web site, according to media reports and a company official. The hacker allegedly used some of the stolen credit card numbers to obtain money for himself.<sup>42</sup>

---

## Challenges Exist in Determining the Link between Data Breaches and Identity Theft

Determining the link between data breaches and identity theft is challenging for several reasons. First, identity theft victims often do not know how their personal information was obtained. According to FTC, in approximately 65 percent of the identity theft complaints it received from October 1, 2005, through August 31, 2006, the victim did not know or report how the information was compromised. Second, victims may misattribute how their data were obtained. For example, federal officials and representatives of a private group that assists victims said that consumers who are notified of a breach often assume that any perceived mistakes on their credit card statements or credit report were a result of the breach. As a result, no government agency maintains comprehensive data on the underlying cause of identity theft. FTC told us that its Identity Theft Data Clearinghouse is limited to self-reported complaints and therefore does not contain statistically reliable information that would allow the agency to determine a link between data breaches and identity theft. Similarly, according to FBI, data maintained by the Internet Crime Complaint Center does not include information sufficient to determine the link between data breaches and identity theft.

---

<sup>42</sup>This breach occurred in December 1999 but was included in the 24 breaches we reviewed because it was reported in the media in January 2000.

---

Third, law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. Finally, conducting comprehensive studies of data breaches and identity theft can be hindered by issues of privacy and confidentiality. For example, companies that have experienced breaches may be unable or unwilling to provide information about affected individuals to researchers.

Some studies conducted by private researchers have sought to determine the extent to which data breaches result in identity theft, but our review found them to contain methodological limitations.<sup>43</sup> One research firm conducted a study of four data breaches, analyzing credit and other application data for suspicious relationships that indicated fraud.<sup>44</sup> The study estimated that no more than 0.10 percent of individuals whose data had been breached experienced resulting identity theft in the form of unauthorized new account creation. However, because the study reviewed only four data breaches, it cannot be considered representative of other breaches. Moreover, two of these breaches did not involve personally identifiable information and thus would not be expected to create a risk of fraud involving new account creation.

Another private research firm surveyed approximately 9,000 individuals about whether they had ever received a notification from an organization about the loss or theft of their personal information.<sup>45</sup> Of the approximately 12 percent of individuals who reported they had received such a notification, 3 percent—or 33 people—said they believed they had suffered identity theft as a result. However, these data are subject to limitations; among other things, individuals are often unaware of whether any fraud they have suffered was, in fact, due to a data breach. A third firm projected in a study that 0.8 percent of consumers whose information a

---

<sup>43</sup> Although we found limitations in how these studies linked data breaches and identity theft, we determined other aspects of these studies to be sufficiently reliable, and we refer to them elsewhere in this report.

<sup>44</sup> ID Analytics, Inc., *National Data Breach Analysis* (2006).

<sup>45</sup> Ponemon Institute, *National Survey* (2005). As noted earlier, this study may also be limited by a low survey response rate.

---

data breach compromised would experience fraud as a result.<sup>46</sup> However, we question the reliability of this estimate, in part because of assumptions made about the number of consumers affected by data breaches.

---

### Type of Data Compromised and Other Factors Influence Potential for Resulting Consumer Harm

The type of data compromised in a breach can effectively determine the potential harm that can result. For example, credit or debit card information such as card numbers and expiration dates generally cannot be used alone to open unauthorized new accounts. Some of the largest and most highly publicized data breaches in recent years largely involved credit or debit card data rather than personally identifiable information. As a result, these breaches put affected consumers at risk of account fraud but not necessarily at risk of fraud involving unauthorized creation of new accounts—the type of identity theft generally considered to have a more harmful direct effect on consumers. While credit and debit card fraud is a significant problem—the FTC estimates it results in billions of dollars in losses annually—existing laws limit consumer liability for such fraud and, as a matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges.<sup>47</sup> In contrast, the unauthorized creation of new accounts—such as using someone else’s identity to open credit card or bank accounts, originate home mortgages, file tax returns, or apply for government benefits—can result in substantial financial costs and other hardships.

In addition to the type of data compromised in a breach, several additional factors can influence the extent to which a breach presents the risk of identity theft. These include the following:

- *Intent.* Breaches that are the result of intentional acts—such as hacking into a server to obtain sensitive data—generally are considered to pose more risk than accidental breaches such as a lost laptop or the

---

<sup>46</sup>Javelin Strategy & Research, *Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses* (Pleasanton, California, August 2006).

<sup>47</sup>For unauthorized credit card charges, consumer liability is limited to a maximum of \$50 per account, 15 U.S.C. § 1643. For unauthorized ATM or debit card transactions, the Electronic Fund Transfer Act limits consumer liability, depending on how quickly the consumer reports the loss or theft of the card. Pub. L. No. 90-321, tit. IX, as added Pub. L. No. 95-630, tit. XX, § 2001, 92 Stat. 3728 (Nov. 10, 1978); 15 U.S.C. § 1693g. Consumers may incur additional costs if they inadvertently pay charges they did not incur. In addition, account fraud can cause inconvenience or temporary hardship—such as losing temporary access to account funds or requiring the cancellation and reactivation of cards and the redirecting of automatic payments and deposits.

---

unintentional exposure of sensitive data on the Internet, according to federal agency officials. However, in some cases, such as the theft of a laptop containing personal information, it may be unknown whether the laptop was stolen for the hardware, the personal data, or both.

- *Encryption.* Encryption—encoding data so that it can only be read by authorized individuals—can in some cases prevent unauthorized access. However, some forms of encryption are more effective than others, and encryption does not necessarily preclude fraudulent use of data—for example, if the key used to unencrypt the data is also compromised.
- *Hardware requirements.* Data that only can be accessed using specialized equipment and software may be less likely to be misused in the case of a breach. For example, some entities that have lost data tapes have stated that criminals would require specific data reading equipment and expertise in how to use it to access the information.
- *Number of records.* Larger breaches may pose a greater overall risk that at least one individual would become a victim of identity theft. At the same time, given the resources needed to commit identity theft, breaches of very large numbers of records may pose less risk to any one individual whose data were compromised.

---

## Breach Notification Requirements Can Serve to Encourage Better Data Security Practices and Alert Consumers, but They Also Present Costs and Challenges

Breach notification requirements have several potential benefits, including creating incentives for entities to improve their data security practices (and thus prevent potential breaches from occurring), allowing affected consumers to take measures to prevent or mitigate identity theft, and serving to respect individuals' basic right to know when their personal information is compromised. At the same time, breach notification requirements present costs, both for developing compliance strategies and for actual notifications in the event of a breach. Further, there is the risk of overnotification, or inundating consumers with frequent notifications of breaches that may present little or no risk of identity theft or other harm. Thus, policymakers face the challenge of setting a notification standard that allows individuals to take steps to protect themselves where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action.

# **Exhibit C**

1 of 12 DOCUMENTS

LEXISNEXIS' CODE OF FEDERAL REGULATIONS  
Copyright © 2007, by Matthew Bender & Company, a member  
of the LexisNexis Group. All rights reserved.

\*\*\* THIS SECTION IS CURRENT THROUGH THE JULY 4, 2007 ISSUE OF \*\*\*  
\*\*\* THE FEDERAL REGISTER \*\*\*

TITLE 12 -- BANKS AND BANKING  
CHAPTER II -- FEDERAL RESERVE SYSTEM  
SUBCHAPTER A -- BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM  
PART 226 -- TRUTH IN LENDING (REGULATION Z)  
SUBPART B -- OPEN-END CREDIT

**Go to the CFR Archive Directory**

*12 CFR 226.12*

§ 226.12 Special credit card provisions.

(a) Issuance of credit cards. Regardless of the purpose for which a credit card is to be used, including business, commercial, or agricultural use, no credit card shall be issued to any person except:

- (1) In response to an oral or written request or application for the card; or
- (2) As a renewal of, or substitute for, an accepted credit card. n21

n21 For purposes of this section, accepted credit card means any credit card that a cardholder has requested or applied for and received, or has signed, used, or authorized another person to use to obtain credit. Any credit card issued as a renewal or substitute in accordance with this paragraph becomes an accepted credit card when received by the cardholder.

(b) Liability of cardholder for unauthorized use -- (1) Limitation on amount. The liability of a cardholder for unauthorized use n22 of a credit card shall not exceed the lesser of \$ 50 or the amount of money, property, labor, or services obtained by the unauthorized use before notification to the card issuer under paragraph (b)(3) of this section.

n22 Unauthorized use means the use of a credit card by a person, other than the cardholder, who does not have actual, implied, or apparent authority for such use, and from which the cardholder receives no benefit.

(2) Conditions of liability. A cardholder shall be liable for unauthorized use of a credit card only if:

- (i) The credit card is an accepted credit card;
- (ii) The card issuer has provided adequate notice n23 of the cardholder's maximum potential liability and of means by which the card issuer may be notified of loss or theft of the card. The notice shall state that the cardholder's liability shall not exceed \$ 50 (or any lesser amount) and that the cardholder may give oral or written notification, and shall describe a means of notification (for example, a telephone number, an address, or both); and

n23 Adequate notice means a printed notice to a cardholder that sets forth clearly the pertinent facts so that the cardholder may reasonably be expected to have noticed it and understood its meaning. The notice may be given by any means reasonably assuring receipt by the cardholder.

(iii) The card issuer has provided a means to identify the cardholder on the account or the authorized user of the card.

(3) Notification to card issuer. Notification to a card issuer is given when steps have been taken as may be reasonably required in the ordinary course of business to provide the card issuer with the pertinent information about the loss, theft, or possible unauthorized use of a credit card, regardless of whether any particular officer, employee, or agent of the card issuer does, in fact, receive the information. Notification may be given, at the option of the person giving it, in person, by telephone, or in writing. Notification in writing is considered given at the time of receipt or, whether or not received, at the expiration of the time ordinarily required for transmission, whichever is earlier.

(4) Effect of other applicable law or agreement. If state law or an agreement between a cardholder and the card issuer imposes lesser liability than that provided in this paragraph, the lesser liability shall govern.

(5) Business use of credit cards. If 10 or more credit cards are issued by one card issuer for use by the employees of an organization, this section does not prohibit the card issuer and the organization from agreeing to liability for unauthorized use without regard to this section. However, liability for unauthorized use may be imposed on an employee of the organization, by either the card issuer or the organization, only in accordance with this section.

(c) Right of cardholder to assert claims or defenses against card issuer n24 -- (1) General rule. When a person who honors a credit card fails to resolve satisfactorily a dispute as to property or services purchased with the credit card in a consumer credit transaction, the cardholder may assert against the card issuer all claims (other than tort claims) and defenses arising out of the transaction and relating to the failure to resolve the dispute. The cardholder may withhold payment up to the amount of credit outstanding for the property or services that gave rise to the dispute and any finance or other charges imposed on that amount. n25

n24 This paragraph does not apply to the use of a check guarantee card or a debit card in connection with an overdraft credit plan, or to a check guarantee card used in connection with cash advance checks.

n25 The amount of the claim or defense that the cardholder may assert shall not exceed the amount of credit outstanding for the disputed transaction at the time the cardholder first notifies the card issuer or the person honoring the credit card of the existence of the claim or defense. To determine the amount of credit outstanding for purposes of this section, payments and other credits shall be applied to: (1) Late charges in the order of entry to the account; then to (2) finance charges in the order of entry to the account; and then to (3) any other debits in the order of entry to the account. If more than one item is included in a single extension of credit, credits are to be distributed pro rata according to prices and applicable taxes.

(2) Adverse credit reports prohibited. If, in accordance with paragraph (c)(1) of this section, the cardholder withholds payment of the amount of credit outstanding for the disputed transaction, the card issuer shall not report that amount as delinquent until the dispute is settled or judgment is rendered.

(3) Limitations. The rights stated in paragraphs (c)(1) and (2) of this section apply only if:

(i) The cardholder has made a good faith attempt to resolve the dispute with the person honoring the credit card; and

(ii) The amount of credit extended to obtain the property or services that result in the assertion of the claim or defense by the cardholder exceeds \$ 50, and the disputed transaction occurred in the same state as the cardholder's current designated address or, if not within the same state, within 100 miles from that address. n26

n26 The limitations stated in paragraph (c)(3)(ii) of this section shall not apply when the person honoring the credit card: (1) Is the same person as the card issuer; (2) is controlled by the card issuer directly or indirectly; (3) is under the direct or indirect control of a third person that also directly or indirectly controls the card issuer; (4) controls the card issuer directly or indirectly; (5) is a franchised dealer in the card issuer's products or services; or (6) has obtained the order for the disputed transaction through a mail solicitation made or participated in by the card issuer.

(d) Offsets by card issuer prohibited. (1) A card issuer may not take any action, either before or after termination of credit card privileges, to offset a cardholder's indebtedness arising from a consumer credit transaction under the relevant credit card plan against funds of the cardholder held on deposit with the card issuer.

(2) This paragraph does not alter or affect the right of a card issuer acting under state or Federal law to do any of the following with regard to funds of a cardholder held on deposit with the card issuer if the same procedure is constitutionally available to creditors generally: obtain or enforce a consensual security interest in the funds; attach or otherwise levy upon the funds; or obtain or enforce a court order relating to the funds.

(3) This paragraph does not prohibit a plan, if authorized in writing by the cardholder, under which the card issuer may periodically deduct all or part of the cardholder's credit card debt from a deposit account held with the card issuer (subject to the limitations in § 226.13(d)(1)).

(e) Prompt notification of returns and crediting of refunds. (1) When a creditor other than the card issuer accepts the return of property or forgives a debt for services that is to be reflected as a credit to the consumer's credit card account, that creditor shall, within 7 business days from accepting the return or forgiving the debt, transmit a credit statement to the card issuer through the card issuer's normal channels for credit statements.

(2) The card issuer shall, within 3 business days from receipt of a credit statement, credit the consumer's account with the amount of the refund.

(3) If a creditor other than a card issuer routinely gives cash refunds to consumers paying in cash, the creditor shall also give credit or cash refunds to consumers using credit cards, unless it discloses at the time the transaction is consummated that credit or cash refunds for returns are not given. This section does not require refunds for returns nor does it prohibit refunds in kind.

(f) Discounts; tie-in arrangements. No card issuer may, by contract or otherwise:

(1) Prohibit any person who honors a credit card from offering a discount to a consumer to induce the consumer to pay by cash, check, or similar means rather than by use of a credit card or its underlying account for the purchase of property or services; or

(2) Require any person who honors the card issuer's credit card to open or maintain any account or obtain any other service not essential to the operation of the credit card plan from the card issuer or any other person, as a condition of participation in a credit card plan. If maintenance of an account for clearing purposes is determined to be essential to the operation of the credit card plan, it may be required only if no service charges or minimum balance requirements are imposed.

(g) Relation to Electronic Fund Transfer Act and Regulation E. For guidance on whether Regulation Z (12 CFR part 226) or Regulation E (12 CFR part 205) applies in instances involving both credit and electronic fund transfer aspects, refer to Regulation E, *12 CFR 205.12(a)* regarding issuance and liability for unauthorized use. On matters other than issuance and liability, this section applies to the credit aspects of combined credit/electronic fund transfer transactions, as applicable.

**HISTORY:** [Reg. Z, 46 FR 20892, Apr. 7, 1981; 65 FR 17129, 17131, Mar. 31, 2000]

**AUTHORITY:** AUTHORITY NOTE APPLICABLE TO ENTIRE PART:  
*12 U.S.C. 3806; 15 U.S.C. 1604 and 1637(c)(5).*

**NOTES:** [EFFECTIVE DATE NOTE: *65 FR 17129, 17131*, Mar. 31, 2000, which revised paragraph (g), effective Mar. 24, 2000, provides: "Compliance is optional until October 1, 2000."]

NOTES APPLICABLE TO ENTIRE TITLE:

CROSS REFERENCES: Farmers Home Administration: See Agriculture, 7 CFR, chapter XVIII.

Office of Assistant Secretary for Housing-Federal Housing Commissioner, Department of Housing and Urban Development: See Housing and Urban Development, 24 CFR, chapter II.

Fiscal Service: See Money and Finance: Treasury, 31 CFR, chapter II.

Monetary Offices: See Money and Finance: Treasury, 31 CFR, chapter I.

Commodity Credit Corporation: See Agriculture, 7 CFR, chapter XIV.

Small Business Administration: See Business Credit and Assistance, 13 CFR, chapter I.

Rural Electrification Administration: See Agriculture, 7 CFR, chapter XVII.

NOTES TO DECISIONS: COURT AND ADMINISTRATIVE DECISIONS SIGNIFICANTLY DISCUSSING SECTION --

*Ives v W. T. Grant Co. (1975, CA2 Conn) 522 F2d 749*

*Citibank v Mincks (2004, Mo App) 135 SW3d 545*

1710 words

# **Exhibit D**

1 of 1 DOCUMENT

LEXISNEXIS' CODE OF FEDERAL REGULATIONS  
Copyright © 2007, by Matthew Bender & Company, a member  
of the LexisNexis Group. All rights reserved.

\*\*\* THIS SECTION IS CURRENT THROUGH THE JULY 4, 2007 ISSUE OF \*\*\*  
\*\*\* THE FEDERAL REGISTER \*\*\*

TITLE 12 -- BANKS AND BANKING  
CHAPTER II -- FEDERAL RESERVE SYSTEM  
SUBCHAPTER A -- BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM  
PART 205 -- ELECTRONIC FUND TRANSFERS (REGULATION E)

**Go to the CFR Archive Directory**

*12 CFR 205.6*

§ 205.6 Liability of consumer for unauthorized transfers.

(a) Conditions for liability. A consumer may be held liable, within the limitations described in paragraph (b) of this section, for an unauthorized electronic fund transfer involving the consumer's account only if the financial institution has provided the disclosures required by § 205.7(b)(1), (2), and (3). If the unauthorized transfer involved an access device, it must be an accepted access device and the financial institution must have provided a means to identify the consumer to whom it was issued.

(b) Limitations on amount of liability. A consumer's liability for an unauthorized electronic fund transfer or a series of related unauthorized transfers shall be determined as follows:

(1) Timely notice given. If the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$ 50 or the amount of unauthorized transfers that occur before notice to the financial institution.

(2) Timely notice not given. If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$ 500 or the sum of:

(i) \$ 50 or the amount of unauthorized transfers that occur within the two business days, whichever is less; and

(ii) The amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period.

(3) Periodic statement; timely notice not given. A consumer must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. If the consumer fails to do so, the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not have occurred had the consumer notified the institution within the 60-day period. When an access device is involved in the unauthorized transfer, the consumer may be liable for other amounts set forth in paragraphs (b)(1) or (b)(2) of this section, as applicable.

(4) Extension of time limits. If the consumer's delay in notifying the financial institution was due to extenuating circumstances, the institution shall extend the times specified above to a reasonable period.

## 12 CFR 205.6

(5) Notice to financial institution. (i) Notice to a financial institution is given when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information.

(ii) The consumer may notify the institution in person, by telephone, or in writing.

(iii) Written notice is considered given at the time the consumer mails the notice or delivers it for transmission to the institution by any other usual means. Notice may be considered constructively given when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized transfer to or from the consumer's account has been or may be made.

(6) Liability under state law or agreement. If state law or an agreement between the consumer and the financial institution imposes less liability than is provided by this section, the consumer's liability shall not exceed the amount imposed under the state law or agreement.

**HISTORY:** [44 *FR* 18480, Mar. 28, 1979, as amended at 44 *FR* 33839, June 13, 1979; 44 *FR* 46434, Aug. 8, 1979; Redesignated and amended at 44 *FR* 59470, Oct. 15, 1979; 48 *FR* 14881, Apr. 6, 1983, 53 *FR* 52653, Dec. 29, 1988; 61 *FR* 19662, 19670, May 2, 1996]

**AUTHORITY:** AUTHORITY NOTE APPLICABLE TO ENTIRE PART:  
15 *U.S.C.* 1693b.

**NOTES:** NOTES APPLICABLE TO ENTIRE TITLE:

CROSS REFERENCES: Farmers Home Administration: See Agriculture, 7 CFR, chapter XVIII.

Office of Assistant Secretary for Housing-Federal Housing Commissioner, Department of Housing and Urban Development: See Housing and Urban Development, 24 CFR, chapter II.

Fiscal Service: See Money and Finance: Treasury, 31 CFR, chapter II.

Monetary Offices: See Money and Finance: Treasury, 31 CFR, chapter I.

Commodity Credit Corporation: See Agriculture, 7 CFR, chapter XIV.

Small Business Administration: See Business Credit and Assistance, 13 CFR, chapter I.

Rural Electrification Administration: See Agriculture, 7 CFR, chapter XVII.